# Consultative Document / Document de consultation

Atomic Energy Control Board / Commission de contrôle de l'énergie atomique

CONSULTATIVE DOCUMENT C-70

Proposed Regulatory Guide

# THE USE OF FAULT TREES IN LICENSING SUBMISSIONS

Issued for comment:

May 31, 1983

Canada

This Consultative Document is issued in order to provide an opportunity for public review of the proposal it contains before formal issue as a Regulatory Document. Comments are encouraged and should be directed to the address below before 1 SEPTEMBER 1983.

Unless otherwise requested by the submittor, a copy of all comments received will be placed in the AECB public documents room.

Direct comments to:

Regulations Development Section
Atomic Energy Control Board
P.O. Box 1046
Ottawa, Ontario
CANADA
K1P 5S9

## THE AECB REGULATORY DOCUMENTS SYSTEM

1. Siting, design, manufacture, construction, commissioning, operation, and decommissioning of nuclear facilities, or the production, possession, use and disposal of prescribed substances, in Canada or under Canadian control, are subject to the provisions of the Atomic Energy Control Act and Regulations administered by the Atomic Energy Control Board (AECB).

2. In addition to the Atomic Energy Control Regulations, three other categories of Regulatory Document are employed by the AECB. These are:

   Generic Licence Conditions - standard sets of conditions that are included in particular AECB licences of a common type, unless specific circumstances indicate otherwise;

   Regulatory Policy Statements - firm expressions that particular "requirements" not expressed as Regulations or Licence Conditions be complied with or that any requirements be met in a particular manner but where the AECB retains the discretion to allow deviations or to consider alternative means of attaining the same objectives where a satisfactory case is made; and

   Regulatory Guides - guidance or advice on any aspect of the AECB's regulatory process that is given in a manner less rigid than that intended by Policy Statements.

3. In developing Regulatory Documents, the AECB publishes its proposals as Consultative Documents in order to solicit comments both from the nuclear industry and from the public. This is done prior to releasing any Regulatory Document in final form. In certain cases, after the period for public comment, a Consultative Document may be issued for "trial use". This is done for a limited period of time to gain practical experience. Following the period of trial use, the revised document is re-issued for further public comment prior to release in final form.

4. Comments on Consultative Documents and suggestions for new Regulatory Documents and for improvement to those that exist are encouraged and should be directed to the Regulations Development Section of the AECB.

5. Copies of Consultative Documents, Regulatory Documents and related index lists are available in both English and French on request from the Office of Public Information. Requests for technical information on and interpretation of documents should be addressed to this office.

6. The Atomic Energy Control Board may be contacted as follows:

   Postal address: Atomic Energy Control Board
   P.O. Box 1046
   Ottawa, Ontario
   CANADA
   K1P 5S9

   Telephone
   General Inquiries: (613) 995-5894

## FOREWORD

The need to gain a better understanding of the risks associated with the operation of increasingly complex nuclear facilities can be satisfied in large measure by the use of the fault tree technique. This technique provides a powerful tool for the presentation, in a precise and logical manner, of the possible ways in which a system can fail. It also permits thorough examination of the design of a facility to identify links between systems whose malfunction could result in a release of radioactive material to the environment, and those systems which are designed to prevent or mitigate the effects of such failures.

This Consultative Document describes a proven procedure for applying this technique. Use of the procedure to identify failure modes in both reliability analyses and safety analyses will enhance the licensee's ability to identify design weaknesses and conflicting design objectives. It will also permit the Atomic Energy Control Board to better understand and appreciate the work done by a licensee. Since it is anticipated that the transmission of such information may, in the future, be by electronic means, a section of the document identifies a suitable format for computer compatibility and for information retrieval.

TABLE OF CONTENTS


| | | |
|---|---|---|
| THE AECB REGULATORY DOCUMENTS SYSTEM | | ii |
| FOREWORD | | iii |
| 1. SCOPE | | 1 |
| 2. GENERAL | | 1 |
| 3. FAULT TREE FUNDAMENTALS | | 2 |
| 4. FAULT TREE FOR SYSTEMS | | 3 |
| 5. FAULT TREE FORMAT | | 5 |
| FAULT TREE SYMBOLS | APPENDIX | A |
| FAULT TREE DESCRIPTION FILE | APPENDIX | B |

REGULATORY GUIDE ON
THE USE OF FAULT TREES IN
LICENSING SUBMISSIONS

1. SCOPE

1.1 The fault tree, as described in this Regulatory Guide, is primarily a tool for proper and formally correct definition of problems to be analysed. Use of the fault tree for numerical evaluation of failures rates and probabilities is considered secondary.

1.2 The objective of this Guide is to standardize the fault tree presentation technique in order to

(a) prevent errors in interpretation of fault trees, especially when the fault tree is used or reviewed by a person other than the originator of the fault tree;

(b) facilitate the use of computer facilities for fault tree processing.

1.3 This Guide should be used whenever information supporting a licence application is submitted to the AECB in the form of a fault tree.

2. GENERAL

2.1 A fault tree is a hierarchically structured graphical representation of system failures and their potential causes. The system failures include in this context all the relevant malfunctions and other concerns which interfere with the proper functioning of a system.

2.2 A fault tree should

(a) identify factors affecting the reliability characteristics of the system. These factors include failure modes, environmental conditions, loss of energy supplies, and other factors causing or contributing to system failures;

(b) identify contradictions in requirements for redundancy and fail-safe design or operation;

(c) identify common events, including those that are

(i) detrimental to the built-in redundancy, or

(ii) linked, either as a cause or a consequence, to a failure or malfunction of another system designed to mitigate the consequences of the first failure or malfunction.

2.3 The fault tree can also serve as a basis for selection and development of procedures for numerical evaluation of reliability characteristics.

2.4 The use of fault trees in a particular application should be determined by considering the following:

(a) The fault tree is recommended for the analysis of complex systems consisting of several cross-linked subsystems which may have contradictory design requirements, especially when the design also requires the involvement of various specialists who may have different sets of priorities.

(b) The fault tree is not recommended for the analysis of simple systems or for systems in which the complexity is caused by multiple applications of identical building blocks.

2.5 The development of fault trees should start at an early stage in design so as to reflect the development of the design and a deepening understanding of the modes of failure. As the final fault trees are likely to be large, it is essential that their format be such that they can be handled with the aid of computers.

## 3. FAULT TREE FUNDAMENTALS

3.1 The top event of the fault tree identifies the most undesirable occurrence in the context of the analysis for which the particular tree is used. Examples of top events include a system malfunction, a failure to achieve a certain goal, or the onset of a dangerous condition.

3.2 Fault trees with multiple top events which share common branches or events are acceptable. Such fault trees are especially useful for the demonstration of contradictions in requirements. An example of such contradictory top events would be "loss of dousing" and "spurious dousing."

3.3 Events in the fault tree are not limited to "faults" but may also denote various happenings, outcomes or conditions that are identified as relevant factors for the occurrence of the top event.

3.4 The fault tree has the form of a diagram in which the events are linked by gates. Each gate has one output event and a number of input events. The input events identify possible causes and conditions for the occurrence of the output event.

3.5 Linking of events through gates expresses causal relation of events as understood by the analyst. Linking of events does not define any time sequencing other than the logical necessity for an event causing a condition to occur before that condition can exist.

3.6 If the output event of a gate defines a failure of a function, the input events to that gate should refer to both hardware malfunctions and performance constraints. If the output event defines a hardware malfunction, the input events should refer to hardware failures, to lack of control, and also to lack of essential supplies (of water, for example) if applicable and not included already as part of performance constraints.

3.7 Hardware failures should include both endogenous failures (due to internal weakness) and exogenous failures (due to damage or other outside effects). The exogenous failures should include effects of all conditions or environments the hardware item can encounter.

3.8 Fault trees should include, where relevant, effects of human error and effects of deficiencies in computer software as events that cause lack of control of particular hardware items.

3.9 Each event in the fault tree must be uniquely identified. Events related to hardware items must be defined in such a way that the corresponding hardware item can be identified in the design documentation.

3.10 If several events in a fault tree represent different failure modes of the same item, these events must be identified in such a way that it is possible to distinguish them as separate and at the same time to recognise them as a group of events related to the same item.

3.11 If the same event (e.g., the failure of a specific valve to close) occurs in several places in a tree, or if it occurs in several trees, all occurrences must bear the same identification even if the occurrences are in separate submissions. However, events which are similar but which involve different components must not bear the same identification.

3.12 The development of a particular fault tree terminates after reaching

(a) events which have been or are to be further developed in another fault tree;

(b) events which the analyst deems unnecessary to further develop at the time of the analysis;

(c) basic events.

3.13 Basic events in a fault tree are those events for which the relevant characteristics

(a) can be defined by other means than a fault tree, and

(b) are not affected by conditions or occurrences having, simultaneously, an effect on other events in the fault tree.

3.14 If a basic event refers to a grouping (assembly) of items, the identification of the event should include a reference to an appropriate parts list (list of items in the grouping).

3.15 Events which the analyst has considered, but excluded from further analysis as non-relevant, should also be included in the fault tree as non-relevant events.

## 4. FAULT TREES FOR SYSTEMS

4.1 Each system for which a fault tree is developed should be defined by a description of the system function and by an identification of the system boundary.

4.2 A description of system function should include

(a) a summary of the design intent;

(b) identification of operating modes;

(c) description of operation in each operating mode including

- performance characteristics defined in physically measurable units
- environmental limits
- expected limits of duration (mission time)
- constraints on maintenance and repair, if any
- list of initiating conditions and operations for transition from one operational mode to another;

(d) list of applicable documents such as drawings, specifications, operating procedures, engineering analyses and engineering data required for a proper understanding of system functions in anticipated conditions.

4.3 The system boundary defines the interaction and interface with other systems. The boundary should be described by identifying the particular functions (e.g., electrical supply of AC 115V/250VA) and the parts (e.g., connection to fuse box 6554-PL125S-S2-012) which form the boundary.

4.4 If the function of the analysed system depends on the function of another system for which a separate fault tree is developed, the fault tree of the analysed system should be terminated with an event referring to the system boundary. This event has to have the same identification as the corresponding event on the fault tree for the system on which the function of the analysed system depends so that the latter fault tree effectively forms a continuation of the former.

4.5 The level of detail required in the description of the system function and in the definition of the system boundary varies according to the stage of system development. However the description should

(a) identify the organization issuing the document and the date of release, and

(b) be subject to a defined process which ensures

- verification that the description of the system function and identification of the system boundary corresponds to the current status of the system or equipment
- that it is possible to define changes to the system which are made after the fault tree has been developed.

4.6 The fault tree for a system should correspond directly with the system description as applicable at the time of designing the fault tree. Some fault trees may be required to be subject to a controlled updating process.

4.7 The fault tree should be developed to represent how different system failure modes can occur. It should not be modified to conform to the mathematical formulas used for eventual numerical evaluation of probabilities and failure rates.

4.8 If the fault tree depicts an impairment caused by an existing failure, a malfunction, or an out-of-service condition of a part of the system, the event describing that failure, malfunction, or out-of-service condition should be included in the fault tree and marked as an event which has already happened.

5. FAULT TREE FORMAT

5.1 Each event in the fault tree should have assigned an event code in accordance with an approved coding scheme. Typically, an event code will consist of three parts:

(a) system identification;

(b) component identification;

(c) failure mode.

5.2 An event description (name) is mandatory for the top event and all events for which the description cannot be derived directly from the description of the corresponding input events and the type of gate used.

5.3 The symbols in the fault tree should be easily distinguishable and should be clearly defined by a standard or a guide acceptable to the AECB. An example of an acceptable standard is shown in Appendix A of this Guide.

5.4 The following practices are recommended:

(a) If the fault tree has multiple top events, they should not be tied together by a dummy (artificial) top event.

(b) Events considered non-relevant should be marked by dashed lines.

5.5 Fault trees may be submitted in the form of a computer file. For large trees the licensee may be required to use that form. The method for transferring the file must be acceptable to the AECB. An acceptable method for transferring the file to the AECB is a transmission of the Fault Tree Description File as defined in Appendix B in this document. The file is transmitted through a direct computer access using the ASCII character set and 300 baud asynchronous modem Bell 103A or equivalent.

5.6 Any submission that makes reference to fault trees submitted in the form of computer files should include or make reference to a list of fault tree description files; the content of each file should be indicated by a short description (heading) and an abridged plot with events in the top three levels of the fault tree that is defined by that file.

APPENDIX A

FAULT TREE SYMBOLS

A.1 The standard orientation of the fault tree is horizontal with the top event on the left. Fault trees with multiple top events are acceptable.

A.2 The symbol for an event consists of

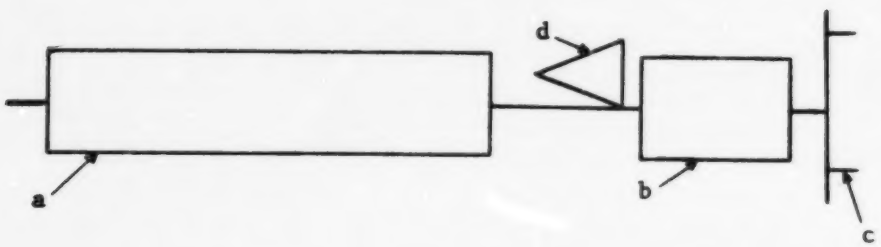
(a) event description box;

(b) event type symbol;

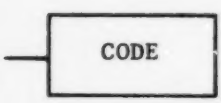
(c) gate input connection line;

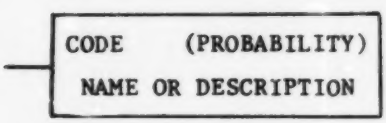
(d) transfer-out symbol (if applicable).

The symbol for an event is drawn by solid lines or dashed lines. All lettering is by solid lines. Use of coloured lines is acceptable.




A.3 The event description box shall contain the event code. It may also contain the event name, and other information such as probability.




A.4 The event type symbols shall be selected from the attached Event Type Symbol Table.

A.5 If an event represents a common cause, it is shown on the fault tree as a set of events linked to whatever event they affect. All events in the set shall

have the same event code and be marked by a symbol (transfer-in), except the last event in the set. The last event in the set is marked by the appropriate terminating symbol, or by the appropriate gate symbol.

A.6 If a fault tree is presented in several sections, an event representing a common cause which appears on two or more of these sections should be treated as follows:

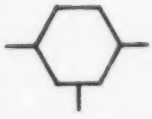
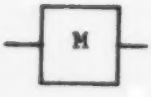
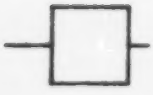
(a) the event should be marked with a terminating symbol or with a gate symbol (if further developed) on only one of the sections;

(b) on the section where the terminating or gate symbol is used, the occurrence of the common event on other sections should be indicated, in the same level as the top event, by an unlinked symbol for a transfer-in event;

(c) on all other sections, the continuation of the event set should be marked by the long-transfer symbol for the last event in the portion of the event set on that section.

## EVENT TYPE SYMBOL TABLE

**Gate Symbols**

| | | |
|---|---|---|
| | AND-gate | Event occurs only if all input events occur simultaneously. |
| | OR-gate | Event occurs if any of the input events occurs, either alone or in any combination with other input events. |
| | Exclusive OR-gate | Event occurs only if one of the input events occurs alone (used typically with two input events). |
| | Fork-gate | Event occurs if any of the input events occurs, but its degree of severity depends on which input event or combination occurred. (Boolean logic is not applicable here.) |
|  | WHILST-gate | Event occurs only if input event attached to the right occurs whilst the event attached to the bottom and forming the condition is in force. If the condition is caused by the occurrence of another event, the WHILST gate implies timing of events. |
| | Redundant Structure | Enclosed numbers indicate level of redundancy. The format is m/n. The event occurs if at least m of the n input events occur. |
|   | Multiplexed Event | Symbol used when all input events are so similar that, for understanding of the fault tree logic, it is sufficient to develop only one of them. The number of inputs must be defined in the event description box. |
|  | Gate (general) | General symbol of a gate. Its meaning must be defined in the event description box. |
| | NOT-gate | Event represents a condition which is the inverse of the condition defined by the input event. |

**Terminating Symbols**

| | | |
|---|---|---|
| | Basic Event | Event which cannot be subdivided. |
| (none) | Basic Condition | Basic event in the conditional branch of a WHILST gate (optional). |
| | Undeveloped Event | Event for which subdivision was not done (usually because it was considered unnecessary). |
| | Analyzed Elsewhere | Event which is further developed on another fault tree. |
| | House | Event which has already happened. |

**Transfer Symbols**

| | | |
|---|---|---|
| | Transfer-in | Event denotes common cause. |
| | Long Transfer | Common event, also used on another fault tree. |

APPENDIX B

## FAULT TREE DESCRIPTION FILE

B.1 The Fault Tree Description File consists of records (cards, lines) with up to 80 columns each. The records are divided into four categories:

(a) skeleton description records;

(b) labelling records;

(c) auxiliary records;

(d) arbitrary records.

Records are in a free format, with character groups separated by at least one blank space. No requirement for sequencing of records exists, except as stated in paragraphs B.4.3, B.5.3 and B.6.

B.2 Each event in the tree is identified by an event code formed by a group of characters taken from the ASCII 64-character set, other than the comma (,) and the asterisk (*) which shall not be used. The ampersand (&), when used as the first character of the code, may be declared a prefix substitute as defined in B.5.3. The maximum length of an event code is 16 characters.

B.3.1 The skeleton description records form the minimum set of records required to describe the fault tree. They include gate description records, basic event description records, and Z-records.

B.3.2 The gate description records have the format

AAAA Gn BBBB CCCC DDD

where

AAAA is the event code of the gate output event;

Gn is the gate identification group, where G represents the type of gate and n represents the number of inputs;

BBBB, etc., are the event codes of gate input events.

Event codes and the type identification group are separated from each other by at least one blank space. The type identifier consists of a character defining the type of gate followed immediately by one or two digits identifying the number of input event codes. Some gate types (e.g., N1 and W2) have a mandatory number of inputs. The gate types are as follows:

An - AND-gate

Fn - FORK-gate

Gn - Gate (general)

Ml - Multiplexed structure

N1 - NOT-gate

Rn - OR-gate

W2 - Whilst-gate

Xn - Exclusive-OR-gate

mn - Redundant structure (both m and n are single digits)

The sequence of input events corresponds to the sequence in which events are plotted from the top down (when the tree axis is horizontal). For W2, the second input event code corresponds to the event identifying the condition.

B.3.3 The basic event description records are required only for modification of the symbol and for numerical data (if used). The format of the basic event description record is

AAAA T #xxx

where

AAAA is the event code of the basic event;

T is the symbol modifier;

#xxx is the data group.

The symbol modifiers define the terminating symbols as follows:

none - circle

D - diamond

E - diamond with circle

H - house (must not be followed by data group).

The symbol modifier is separated from the event code by at least one blank space.

The data group, if used, starts with a number sign (#) which is separated from the symbol modifier, or from the event code if no symbol modifier is used, by at least one blank space. The formats for data are as follows:

(a) Group 1 data (dimension time$^{-1}$):

The failure rate is defined in failures per unit of time (e.g., 1.5/Y or 2E-6/H), as time between failures (e.g., 75Y), or in bits (B) ($10^{-6}$ per hour, e.g., 114.7B) or fits (F) ($10^{-9}$ per hour, e.g., 25F). The format of the number is either decimal (e.g., 0.02 or .02) or exponential (e.g., 3.5E-05). The number of digits after the decimal point should not exceed four since a truncation may commence at the fifth place.

The units of time are Y for year, D for day, and H for hour. The number and letter, or the number, slash and letter must form a single group, without spaces.

(b) Group 2 data (dimensionless) may have any one of the following formats:

Probability: a real number between zero and one, either in decimal or exponential format as defined above.

Probability of failure within time T: defined by failure rate as stated above, followed by the key word FOR and the duration of the time period (mission time). The key word is separated by spaces. The time duration has the same format as the mean time between failures defined above.

Unavailability: defined either by a single number (see probability) or by failure rate in any of the forms specified above, followed by mean time to repair (e.g., 2.5/Y 0.3H or 15Y 2.5D).

Which group of data is required depends on the composition of the fault tree logic.

B.3.4 Z-records identify events which should be plotted by dotted lines. The format of the record is

AAAA Z

where

AAAA is the event code, and

Z is an identifier separated from the event code by at least one blank space.

B.3.5 If colour plotting is used, the colours and other attributes may be defined by a group of characters following a dot (.) as a group identifier. The meaning of the characters would depend on the particular application.

B.4.1 The labelling records include event name records, title records, and records with notes to basic events. Although not all events must be labelled, a sufficient number of labelling records shall be included in the fault tree description file to assure that the fault tree can be properly understood. For M1 gates an event name record is mandatory.

B.4.2 The event name record has the format

AAAA 'xxxx xx xxx;zz z zzzz

where

AAAA is the event code;

the apostrophe (') is separated from the event code by at least one blank space;

xxxx xx xxx is the first line of the event name.

The event name (description) starts immediately after the apostrophe and may contain up to 40 printable ASCII characters. The semi-colon (;) is used to terminate the first line on plots where the name is plotted on two lines with a maximum of 20 characters each.

B.4.3 The title record identifying the title has the same format as the event name record; it is distinguished by its placement before any labelling record or skeleton description record. The event code on the title record may be either the code of an event in the fault tree (in which case the title record serves simultaneously as a name record for that event), or a dummy code, used just to satisfy the format requirements.

B.4.4 The record with a note to a basic event has the same format as the event name record, but uses as identifier a colon (:) instead of an apostrophe (').

B.5.1 Auxiliary records facilitate the handling of the fault tree description file, including input, processing, and storing in the fault tree data base. Auxiliary records include comments and records with prefix substitutes.

B.5.2 A record with an asterisk (*) in the first column is considered a comment and is not used in processing of the fault tree. Comments which precede the first processed record are displayed on the terminal during interactive processing, or are inserted in front of the output file if the fault tree is processed in a batch mode.

B.5.3 A prefix substitute definition record consists of an ampersand (&) in the first column followed, after at least one blank space, by an equal sign (=), which is in turn followed by two to six characters identifying the prefix. On subsequent records, in references to events containing that prefix, the prefix can be replaced by an ampersand (&) used as the first character. To form the complete code, the computer replaces the prefix substitute by the defined group of two to six characters. The prefix substitute may be redefined by a new record defining a prefix substitute, or it may be cancelled by a record with blank spaces after the equal sign.

B.6 Arbitrary records include job control cards required by some computer installations, and records with additional information required by some fault tree processing programs, such as definition of program options. Arbitrary records must consist of either a single group of characters, or two or more groups, the first of which must contain a comma (,). Sequencing of arbitrary records depends on the requirement of the program for which they are intended. Files submitted to the AECB may include arbitrary records, without any significance attached to them.

B.7 The following combination records may be used to facilitate handling of the fault tree description file:

(a) Z-record combined with event name record (B.4.1) where Z shall be between the event code and the apostrophe ('), separated by at least one blank space:

AAAA Z 'xxx xx xxx'zzzz z zz

(b) Z-record combined with basic event description record (B.3.3) where Z shall follow the symbol identifier, separated by at least one blank space:

AAAA T Z #xxx

(c) Basic event description record (including combination with Z-record as defined above) combined with name record:

AAAA T Z #xxx 'xxx xx xxxx;zzzz z zz

B.8 If some fault tree analysis programs require additional data, the data may be input by a data group using a dash (-) or a percent sign (%) as an identifier. The format is similar to that of a name record. Those special data groups must not contain an apostrophe (') or a colon (:), and on combination records they must precede the name or comment.

# Consultative Document / Document de consultation

Atomic Energy Control Board / Commission de contrôle de l'énergie atomique

**DOCUMENT DE CONSULTATION C-70**

**Projet de guide de réglementation**

**L'UTILISATION DES ARBRES DE DÉFAILLANCES POUR LA PRÉSENTATION DES DEMANDES DE PERMIS**

**Publication:**

**le 31 mai 1983**

Canada

Ce document de consultation est publié dans le but de fournir au public l'occasion d'examiner le projet de réglementation avant qu'il soit adopté dans sa forme définitive. Vous êtes invités à faire parvenir vos commentaires à l'adresse ci-dessous avant le 1er SEPTEMBRE 1983.

Sauf avis contraire de la part de l'envoyeur, une copie de tous les commentaires reçus sera placée dans la salle des documents officiels aux bureaux de la CCEA.

Prière d'adresser vos commentaires à:

Section, Développement des règlements
Commission de contrôle de l'énergie atomique
C.P. 1046
Ottawa (Ontario)
CANADA
K1P 5S9

## TEXTES DE RÉGLEMENTATION DE LA CCEA

1. Le choix d'emplacement, la conception, la fabrication, la construction, la mise en service, l'exploitation et le déclassement d'installations nucléaires ou la production, la possession, l'utilisation et l'élimination de substances prescrites, au Canada ou sous contrôle canadien, sont assujettis aux dispositions de la Loi sur le contrôle de l'énergie atomique et de son Règlement d'application, dont l'administration relève de la Commission de contrôle de l'énergie atomique (CCEA).

2. En plus du Règlement susmentionné, la CCEA utilise trois catégories de textes de réglementation. En voici une courte description.

   Conditions générales d'autorisation de permis - ensemble de conditions types figurant dans tous les permis similaires délivrés par la CCEA, à moins de circonstances exceptionnelles;

   Déclarations de principe en matière de réglementation - déclarations laissant clairement entendre que certaines "exigences" qui ne figurent ni dans le Règlement ni dans les conditions des permis sont obligatoires ou que certaines exigences doivent être respectées d'une façon déterminée laissant également entendre que la CCEA se réserve le droit de permettre des écarts ou d'envisager d'autres façons d'en arriver aux mêmes fins, lorsque ces façons semblent convenir; et

   Guides de réglementation - directives ou conseils donnés sur tout aspect de la réglementation assurée par la CCEA mais formulés de façon moins rigoureuse que dans les déclarations de principe.

3. Lors de l'élaboration de ses textes de réglementation, la CCEA en publie d'abord le projet à titre de Document de consultation, afin de connaître les commentaires du secteur nucléaire et du grand public, avant que le projet de texte de réglementation paraisse sous sa forme définitive. Dans certains cas, après l'achèvement de la période réservée aux commentaires, la Commission peut faire mettre le document de consultation à l'essai pratique pour un temps limité. Après cette période d'essai, on demande encore une fois l'opinion du public, avant que le document révisé soit publié sous sa forme définitive.

4. Tout commentaire sur les documents de consultation et toute suggestion à l'égard des nouveaux textes de réglementation ou ceux déjà en vigueur sont les bienvenus; il suffit de les transmettre à la Section du développement des règlements de la CCEA.

5. On peut se procurer des exemplaires des documents de consultation et des textes de réglementation, dans les deux langues officielles, en s'adressant au Bureau d'information publique. Toute demande de renseignements techniques ou d'interprétation des textes devrait être acheminée au Bureau susmentionné.

6. L'adresse de la CCEA est la suivante:

   Commission de contrôle de l'énergie atomique
   C.P. 1046
   Succursale "B"
   OTTAWA (Ontario)
   CANADA K1P 5S9

   Renseignements: (613) 995-5894

SOMMAIRE

La technique de l'arbre de défaillances est une méthode qui permet de mieux comprendre, dans une large mesure, les risques qui accompagnent l'exploitation des installations nucléaires sans cesse plus complexes. Grâce à cette technique, on peut présenter de façon précise et logique les diverses possibilités de défaillances d'un système. Cet arbre permet également d'examiner la conception d'une installation afin d'identifier les relations entre les systèmes dont la défaillance peut entraîner le rejet de matières radioactives dans l'environnement et les systèmes qui sont conçus pour prévenir ou atténuer les effets de telles défaillances.

Le présent document de consultation décrit une procédure éprouvée pour mettre en oeuvre cette technique. Son utilisation pour déceler les modes de défaillance dans les analyses de fiabilité et de sûreté permet au détenteur de permis de mieux identifier les faiblesses de conception de même que les objectifs de conception discordants. La procédure permet également à la Commission de contrôle de l'énergie atomique de mieux comprendre et évaluer le travail effectué par le détenteur de permis. Comme il est à prévoir que la transmission de tels renseignements se fera à l'avenir par un moyen électronique, une section du présent document propose un format de présentation adapté à l'ordinateur et à la recherche informatisée.

TABLE DES MATIÈRES


| | |
|---|---|
| TEXTES DE RÉGLEMENTATION DE LA CCEA | ii |
| SOMMAIRE | iii |
| 1. PORTÉE | 1 |
| 2. GÉNÉRALITÉS | 1 |
| 3. ASPECTS FONDAMENTAUX D'UN ARBRE DE DÉFAILLANCES | 2 |
| 4. REPRÉSENTATION DE SYSTÈMES AU MOYEN D'ARBRES DE DÉFAILLANCES | 4 |
| 5. PRÉSENTATION DE L'ARBRE DE DÉFAILLANCES | 5 |
| SYMBOLES DES ARBRES DE DÉFAILLANCES | ANNEXE A |
| FICHIER DE DESCRIPTION D'ARBRES DE DÉFAILLANCES | ANNEXE B |

GUIDE D'UTILISATION DES ARBRES DE DÉFAILLANCES
POUR LA PRÉSENTATION DES DEMANDES DE PERMIS

1. PORTÉE

1.1 L'arbre de défaillances décrit dans le présent guide de réglementation est avant tout un outil qui permet une définition appropriée et formellement correcte des problèmes à analyser. L'utilisation de l'arbre de défaillances pour obtenir une valeur numérique des taux de défaillance et des probabilités constitue un objectif secondaire.

1.2 Le présent guide a pour but de normaliser la technique de présentation de l'arbre de défaillances afin

(a) d'éviter les erreurs d'interprétation surtout lorsque les arbres de défaillances sont utilisés ou examinés par une personne autre que leur créateur;

(b) de faciliter l'utilisation de l'ordinateur dans le traitement des arbres de défaillances.

1.3 Les prescriptions du présent guide devraient être observées lors d'une demande de permis, chaque fois que l'on soumet des informations à la CCEA sous la forme d'un arbre de défaillances.

2. GÉNÉRALITÉS

2.1 Un arbre de défaillances est une présentation graphique et hiérarchique des défaillances d'un système et de leurs causes probables. Dans le présent contexte, sont incluses comme défaillances du système, les pannes et autres problèmes qui entravent le bon fonctionnement du système.

2.2 Un arbre de défaillances devrait

(a) indiquer les facteurs qui influent sur les caractéristiques de fiabilité du système, tels que les modes de défaillance, l'environnement, les pertes en alimentation d'énergie et les autres facteurs causant directement ou indirectement des défaillances du système;

(b) identifier les discordances entre les exigences portant sur la redondance et la sûreté intégrée de la conception ou du fonctionnement;

(c) reconnaître les événements communs, y compris ceux qui sont

(i) préjudiciables à la redondance intégrée, ou

(ii) reliés (comme cause ou conséquence) à la défaillance ou à la panne d'un autre système conçu pour atténuer les conséquences d'une première défaillance ou panne.

2.3 L'arbre de défaillances peut servir également de base au choix et à l'élaboration d'évaluations chiffrées des caractéristiques de fiabilité.

2.4 L'emploi d'arbres de défaillances dans une application particulière devrait répondre aux conditions suivantes:

(a) On recommande d'utiliser un arbre de défaillances dans l'analyse de systèmes complexes dotés de plusieurs sous-systèmes interreliés, mais parfois discordants du point de vue des exigences de conception, particulièrement lorsque la conception est confiée à divers spécialistes qui s'appuient sur des ensembles de priorités différents.

(b) On ne recommande pas d'utiliser un arbre de défaillances pour analyser des systèmes simples ou des systèmes dont la complexité résulte de l'utilisation répétitive des mêmes éléments constitutifs.

2.5 L'élaboration d'arbres de défaillances devrait commencer dès le début de la phase de conception, de façon à refléter le progrès dans la conception et la compréhension des modes de défaillance. Comme il est à prévoir que, en dernier ressort, les arbres de défaillances seront de grandes dimensions, il est essentiel qu'ils se conforment à une présentation compatible avec l'ordinateur.

3. ASPECTS FONDAMENTAUX D'UN ARBRE DE DÉFAILLANCES

3.1 L'événement de tête de l'arbre de défaillances identifie l'incident le plus indésirable dans le contexte de l'analyse pour laquelle on se sert de cet arbre en particulier. Parmi les événements de tête, il faut compter la panne d'un système, l'incapacité d'atteindre un objectif ou le début d'une condition dangereuse.

3.2 On admet les arbres de défaillances ayant plusieurs événements de tête qui partagent les mêmes embranchements ou les mêmes événements. Ces arbres de défaillances sont particulièrement utiles pour mettre en lumière les contradictions entre plusieurs exigences. Une "panne du système d'aspersion" et un "déclenchement inopiné du système d'aspersion" représentent un bon exemple d'événements de tête contradictoires.

3.3 Les événements d'un arbre de défaillances ne sont pas seulement des "défaillances", mais peuvent être aussi bien des faits, des résultats ou des conditions reconnus comme facteurs propices à l'apparition d'un événement de tête.

3.4 L'arbre de défaillances est illustré par un diagramme dans lequel les événements sont reliés par des portes. Chaque porte comprend un certain nombre d'événements d'entrée et un événement de sortie. Les événements d'entrée correspondent aux causes et aux conditions possibles provoquant l'événement de sortie.

3.5 La liaison des événements au moyen de portes représente la relation causale entre les événements, telle que comprise par l'analyste. La liaison des événements n'est soumise à aucune contrainte chronologique autre que l'évidence logique qu'un événement donnant naissance à une condition doit survenir avant la présence de cette condition.

3.6 Si l'événement de sortie d'une porte correspond au défaut de réalisation d'une fonction, les événements d'entrée de cette porte doivent renvoyer aux pannes d'équipement et aux contraintes de rendement correspondantes. Si l'événement de sortie est une panne d'équipement, les événements d'entrée devraient renvoyer aux défaillances d'équipement, aux défauts de réglage et, le cas échéant, au manque d'approvisionnement essentiel, en eau par exemple, si ce manque d'approvisionnement n'est pas déjà inclus dans les contraintes de rendement.

3.7 Dans les pannes d'équipement, on englobe les pannes endogènes (dues à des faiblesses internes) et les pannes exogènes (dues à des dommages extérieurs ou à d'autres effets semblables). On devrait inclure dans les pannes exogènes les effets de toutes les conditions ou de tous les contextes qui peuvent se répercuter sur l'équipement.

3.8 Les arbres de défaillances devraient également englober, lorsque cela s'impose, les effets des erreurs humaines et des déficiences du logiciel informatique, et les considérer comme des événements provoquant un manque de réglage des composants particuliers de l'équipement.

3.9 Chaque événement de l'arbre de défaillances devrait avoir une désignation non équivoque. Les événements liés à l'équipement devraient être définis de telle sorte que la pièce d'équipement correspondante soit bien identifiée dans la documentation de conception.

3.10 Si plusieurs événements d'un arbre de défaillances représentent différents modes de défaillance du même composant, on doit les désigner de telle façon qu'il soit possible de les distinguer les uns des autres, sans perdre de vue que c'est un groupe d'événements liés au même composant.

3.11 Si le même événement (par exemple, le défaut d'une soupape en particulier de se refermer) se produit à plusieurs endroits dans un même arbre ou se produit dans plusieurs arbres, toutes les apparitions de cet événement doivent avoir la même désignation même si celles-ci figurent dans des documents séparés. Toutefois, les événements analogues qui font intervenir des composants différents ne doivent pas avoir la même désignation.

3.12 L'élaboration de l'arbre de défaillances se termine lorsqu'on est parvenu à

(a) des événements qui ont été ou seront élaborés plus en détail dans un autre arbre de défaillances;

(b) des événements que l'analyste ne juge pas nécessaire d'élaborer plus en profondeur au moment de l'analyse;

(c) des événements de base.

3.13 On entend par événements de base d'un arbre de défaillances les événements dont les caractéristiques

(a) peuvent être définies par d'autres moyens que l'arbre de défaillances, et

(b) ne sont pas influencées par des conditions ou des incidents ayant en même temps un effet sur d'autres événements de l'arbre de défaillances.

3.14 Si un événement de base correspond à un groupe de composants, la désignation de l'événement devrait inclure la référence à une liste d'éléments appropriée (liste des composants du groupe).

3.15 Les événements que l'analyste a étudiés, mais qu'il n'a pas cru bon d'analyser plus à fond parce qu'il n'en sentait pas la pertinence, devraient également être incorporés à l'arbre de défaillances sous la désignation d'événements non pertinents.

4. REPRÉSENTATION DE SYSTÈMES AU MOYEN D'ARBRES DE DÉFAILLANCES

4.1 Chaque système auquel on fait correspondre un arbre de défaillances devrait être défini par une description de la fonction du système et une identification de ses limites.

4.2 Une description de la fonction du système devrait comprendre

(a) un résumé de l'intention de la conception;

(b) une désignation des modes de fonctionnement;

(c) une description du fonctionnement de chacun de ces modes comprenant

- des caractéristiques de rendement exprimées en unités physiques mesurables
- des limites sur l'environnement
- des limites de durée prévues (durée de la mission)
- des contraintes sur la maintenance et les réparations, s'il y a lieu
- une liste des conditions et des opérations qui commandent la transition entre un mode de fonctionnement et un autre;

(d) une liste des documents pertinents comme les dessins, les spécifications, la marche à suivre, les analyses et les données techniques nécessaires pour bien comprendre les fonctions du système dans des conditions anticipées.

4.3 Les limites du système définissent l'interaction et l'interface avec d'autres systèmes. On devrait décrire les limites en identifiant les fonctions particulières (par exemple, l'alimentation électrique en CA 115V/250VA), de même que les éléments qui constituent ces limites (par exemple, le raccordement à la boîte à fusibles 6554-PL125S-32-012).

4.4 Si la fonction correspondant au système analysé dépend de la fonction d'un autre système pour lequel on a déjà élaboré un arbre de défaillances distinct, le dernier événement de l'arbre de défaillances du système analysé devrait renvoyer à la limite du système. La désignation de cet événement doit être la même que celle de l'événement correspondant de l'autre arbre de défaillances déjà élaboré, de sorte que le dernier arbre de défaillances soit effectivement le prolongement du premier.

4.5 La quantité de détails nécessaires à la description de la fonction du système et à la définition de ses limites dépend de l'étape de développement du système. Toutefois cette description devrait

(a) indiquer l'organisme qui a produit le document et la date d'émission du document, et

(b) être assujettie à un procédé particulier de sorte que

- l'on puisse vérifier que la description de la fonction du système et l'identification de ses limites correspondent à l'état actuel du système ou de l'équipement
- l'on puisse définir les changements apportés au système après l'élaboration de l'arbre de défaillances.

4.6 L'arbre de défaillances d'un système devrait correspondre directement à la description du système valable au moment de la conception de l'arbre de défaillances. Certains arbres devront faire l'objet de mises à jour contrôlées.

4.7 L'arbre de défaillances devrait être élaboré de façon à représenter la manière dont peuvent se produire les différents modes de défaillance. En aucun cas, il ne devrait être modifié pour concorder avec les formules mathématiques utilisées dans l'évaluation numérique des probabilités et des taux de défaillance.

4.8 Si l'arbre de défaillances décrit une panne due à l'existence d'une défaillance, d'une défectuosité ou de toute mise hors service d'un composant du système, l'événement décrivant cette panne, cette défectuosité ou cette mise hors service doit être inclus dans l'arbre de défaillances et désigné comme un événement qui s'est déjà produit.

## 5. PRÉSENTATION DE L'ARBRE DE DÉFAILLANCES

5.1 A chaque événement de l'arbre de défaillances devrait correspondre un code élaboré d'après un codage approuvé. Généralement, un code d'événements se compose de trois parties:

(a) une désignation du système;

(b) une désignation du composant;

(c) un mode de défaillance.

5.2 Il faut faire correspondre une description d'événement (un nom) à l'événement de tête de même qu'à tous les événements dont la nature n'est pas évidente d'après l'examen des événements d'entrée et du type de portes utilisé.

5.3 Les symboles utilisés dans l'arbre de défaillances devraient se distinguer facilement et devraient être clairement définis par une norme ou un guide acceptable aux yeux de la CCEA, comme la norme qui figure à l'annexe A du présent guide.

5.4 On recommande d'adopter les pratiques suivantes:

(a) Si un arbre de défaillances comporte plusieurs événements de tête, ceux-ci ne devraient pas être regroupés sous un événement de tête factice (artificiel).

(b) Les événements qualifiés de non pertinents devraient être tracés en lignes brisées.

5.5 Les arbres de défaillances peuvent être présentés à la CCEA sous la forme d'un fichier d'ordinateur. Dans le cas des arbres de grandes dimensions, il se peut que le détenteur de permis y soit contraint. La méthode de transmission du fichier doit recevoir l'accord de la CCEA. Une méthode acceptable de transmettre le fichier à la CCEA est de lui faire parvenir le Fichier de description d'arbre de défaillances, tel que défini à l'annexe B du présent document. La transmission se fait par l'intermédiaire d'un accès direct à l'ordinateur utilisant un ensemble de caractères ASCII et un modem asynchrone de 300 bauds, modèle Bell 103A ou l'équivalent.

5.6 Tout document qui fait référence à des arbres de défaillances présentés sous la forme de fichiers d'ordinateur devrait comprendre ou indiquer en référence une liste des fichiers de description d'arbres de défaillances contenant un court résumé de chaque fichier (en-tête) et un tracé sommaire qui se limite aux événements des trois premiers niveaux de l'arbre de défaillances.

ANNEXE A

SYMBOLES DES ARBRES DE DÉFAILLANCES

A.1 L'arbre de défaillances est normalement horizontal et l'événement de tête se trouve à gauche. On admet les arbres de défaillances ayant plusieurs événements de tête.

A.2 Le symbole d'un événement est constitué

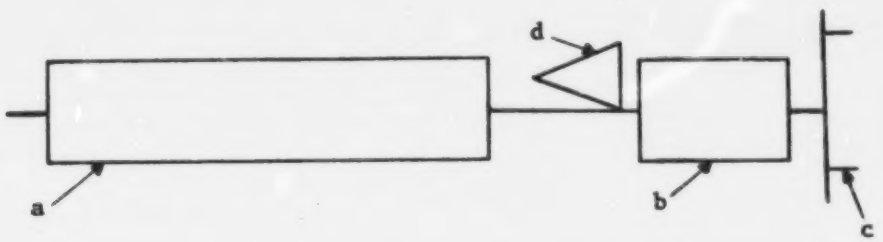
(a) d'une case de description de l'événement;

(b) d'un symbole du type d'événements;

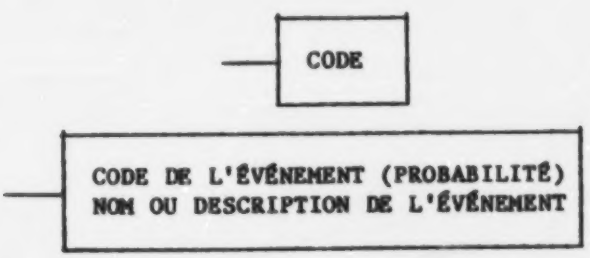
(c) d'une ligne de jonction de l'entrée de la porte;

(d) d'un symbole de transfert externe, s'il y a lieu.

Le symbole d'un événement est tracé en traits pleins ou brisés. Toutes les lettres sont en traits pleins. Il est permis d'utiliser des traits de couleur.




A.3 La case de description de l'événement doit contenir le code de l'événement. Elle peut également contenir le nom de l'événement ou d'autres renseignements comme la probabilité.




A.4 Les symboles des types d'événements doivent être tirés de la Table des symboles de types d'événements qui suit.

A.5 Si un événement représente une cause commune, on l'illustre dans l'arbre de défaillances par un ensemble d'événements reliés à tout événement qu'ils influencent. Tous les événements de l'ensemble doivent avoir le même code d'événement et être repérés par un symbole (transfert interne), sauf pour le dernier événement de l'ensemble que l'on indique par le symbole de fin ou le symbole de porte approprié.

A.6 Si un arbre de défaillances comprend plusieurs sections, un événement représentant une cause commune à deux sections au moins doit être traité comme suit:

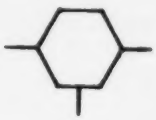
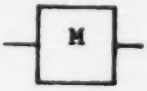
(a) l'événement doit être indiqué par un symbole de fin ou un symbole de porte (s'il est décomposé) sur seulement une des sections;

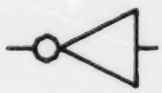
(b) sur la section où l'on utilise le symbole de fin ou le symbole de porte, la présence de l'événement commun sur d'autres sections devrait être indiquée par un symbole non lié, au même niveau que l'événement de tête et correspondant à un événement de transfert interne;

(c) sur toutes les autres sections, le prolongement de l'ensemble d'événements doit être indiqué par le symbole de transfert externe dans le dernier événement de la partie de l'ensemble d'événements de cette section.

## TABLE DES SYMBOLES DE TYPES D'ÉVÉNEMENTS

**Symboles de portes**

| | |
|---|---|
| porte ET | L'événement n'a lieu que si tous les événements d'entrée ont lieu en même temps. |
| porte OU | L'événement a lieu si au moins un des événements d'entrée se produit, que ce soit de façon isolée ou en combinaison avec d'autres événements d'entrée. |
| porte de disjonction | L'événement se produit si seulement un des événements d'entrée se produit (utilisée généralement avec deux événements d'entrée). |
| porte à fourchette | L'événement se produit si l'un des événements d'entrée a lieu; toutefois l'intensité de l'événement de sortie est fonction de l'événement d'entrée qui s'est produit ou de la combinaison d'événements d'entrée qui se produisent. (La logique booléenne ne s'applique pas ici.) |
|  porte à condition | L'événement se produit seulement si l'événement d'entrée qui arrive par la droite se produit pendant que l'événement qui arrive par la base et qui établit la condition est en cours. Si la condition résulte de l'apparition d'un autre événement, la porte à condition signifie la synchronisation des événements. |
| structure redondante | Les chiffres dans la case indiquent le niveau de redondance. Le format d'écriture est m/n. L'événement se produit si au moins m des n événements d'entrée se produisent. |
|   événement multiplexé | Ce symbole est employé lorsque tous les événements d'entrée sont si semblables qu'il suffit de n'en décomposer qu'un seul pour comprendre la logique de l'arbre de défaillances. Le nombre d'entrées doit être défini dans la case de description d'événement. |

| | | |
|---|---|---|
| | porte (générale) | Symbole général de porte dont la signification doit être définie dans la case de description d'événement. |
|  | porte NON | L'événement représente une condition qui est l'inverse de la condition définie par l'événement d'entrée. |

Symboles de fin

| | | |
|---|---|---|
| | événement de base | Événement qui ne peut être décomposé. |
| (néant) | condition de base | Événement de base dans le branchement conditionnel d'une porte à condition (facultatif). |
| | événement non décomposé | Événement que l'on n'a pas décomposé, généralement parce qu'on juge inutile de le faire. |
| | analysé ailleurs | Événement qui est décomposé dans un autre arbre de défaillances. |
| | maison | Événement qui s'est déjà produit. |

Symboles de transfert

| | | |
|---|---|---|
| | transfert interne | Événement représentant une cause commune. |
| | transfert externe | Événement commun, utilisé également dans un autre arbre de défaillances. |

ANNEXE B

FICHIER DE DESCRIPTION D'ARBRES DE DÉFAILLANCES

B.1 Le Fichier de description d'arbres de défaillances est constitué d'enregistrements (cartes, lignes) ayant jusqu'à 80 colonnes chacun. Il y a quatre catégories d'enregistrements:

(a) enregistrements de description de base;

(b) enregistrements de désignation;

(c) enregistrements auxiliaires;

(d) enregistrements arbitraires.

Ces enregistrements se présentent sous format non imposé, mais les groupes de caractères sont séparés par au moins un espace. Ces enregistrements n'ont pas à respecter un ordre quelconque, sauf pour les prescriptions des paragraphes B.4.3, B.5.3 et B.6.

B.2 Chaque événement de l'arbre est désigné par un code d'événements formé d'un groupe de caractères tirés des 64 caractères ASCII, sauf la virgule (,) et l'astérisque (*) qu'il ne faut pas utiliser. L'esperluète (&), lorsqu'elle est utilisée comme premier caractère du code, peut être définie comme substitut de préfixe, conformément à la section B.5.3. La longueur maximale est de 16 caractères.

B.3.1 Les enregistrements de description de base constituent l'ensemble minimal d'enregistrements nécessaires pour décrire l'arbre de défaillances. Ils comprennent les enregistrements de description de portes, les enregistrements de description d'événements de base et les enregistrements Z.

B.3.2 Les enregistrements de description de portes se présentent ainsi:

AAAA Gn BBBB CCCC DDDD

où

AAAA représente le code de l'événement de sortie de la porte;

Gn représente le groupe d'identification de la porte, où G représente le type de portes et n représente le nombre d'entrées;

BBBB, etc., représentent les codes des événements d'entrée de la porte.

Les codes d'événements et le groupe d'identification de porte sont séparés par au moins un espace. L'identificateur de porte se compose d'un caractère définissant le type de portes, suivi immédiatement d'un ou deux chiffres qui indiquent le nombre de codes d'événements d'entrée. Certains types de portes (par ex. N1 et W2) ont un nombre obligatoire d'événements d'entrée. Les types de portes sont les suivants:

An - Porte ET

Fn - Porte à fourchette

Gn - Porte générale

Ml - Structure multiplexée

Nl - Porte NON

Rn - Porte OU

W2 - Porte à condition

Xn - Porte de disjonction

mn - Structure redondante (m et n sont des chiffres indépendants)

L'ordre des événements d'entrée correspond aux événements de haut en bas de l'arbre lorsque l'axe est horizontal. Pour la porte W2, le deuxième code d'événements d'entrée correspond à l'événement qui définit la condition.

B.3.3 Les enregistrements de description d'événements de base ne servent qu'à la modification du symbole et aux données numériques (lorsqu'on en utilise). L'enregistrement de description d'événements de base se présente comme suit:

AAAA T #xxx

où

AAAA représente le code d'événement de l'événement de base;

T représente le modificateur de symbole;

#xxx représente le groupe de données.

Les modificateurs de symbole définissent ainsi les symboles de fin:

aucun - cercle ou ovale

D - losange

E - losange avec cercle

H - maison (ne doit pas être suivi d'un groupe de données).

Le modificateur de symbole est séparé du code d'événements par au moins un espace.

Le groupe de données, s'il y en a un, débute par le signe numéro (#) séparé lui-même par au moins un espace du modificateur de symbole ou du code d'événements, s'il n'y a pas de modificateur de symbole. Voici les formats de données:

(a) Données du groupe 1 (dimension inverse du temps):

Le taux de défaillance est défini en défaillances par unité de temps (par ex. 1.5/Y ou 2E-6/H), en durée entre défaillances (par ex. 75Y), en bits (B) ($10^{-6}$ par heure, par ex. 114.7B) ou en ajustements (F) ($10^{-9}$ par heure, par ex. 25F). Le chiffre du groupe est exprimé soit sous forme décimale (par ex. 0.02 ou .02), soit sous forme exponentielle (par ex. 3.5E-05). Le nombre de chiffres après le point décimal ne devrait pas dépasser quatre, puisque la troncation peut commencer à la cinquième position. Les unités de temps sont: Y (année), D (jour) et H (heure). Le chiffre et la lettre, ou le chiffre, la barre oblique et la lettre ne doivent former qu'un seul groupe sans espace.

(b) Données du groupe 2 (sans dimension) peuvent avoir l'un quelconque des formats suivants:

Probabilité: nombre réel compris entre zéro et un, sous forme décimale ou exponentielle telle que définie précédemment.

Probabilité de défaillance pendant la durée T: définie par un taux de défaillance (comme on l'a déjà indiqué) suivi du mot-clé FOR et de la durée de la période (durée de la mission). Le mot-clé est séparé par des espaces. La durée est écrite sous la même forme que le temps moyen entre défaillances décrit ci-dessus.

Indisponibilité: définie soit par un seul nombre (voir probabilité) ou par un taux de défaillance exprimé dans l'une des formes précisées ci-dessus, et suivi par le temps moyen de reprise (par ex. 2.5/Y 0.3H ou 15Y 2.5D).

Le groupe de données qu'il faut choisir est fonction de la logique de l'arbre de défaillances.

B.3.4 Les enregistrements Z indiquent les événements qui devraient être tracés en lignes brisées. La présentation de l'enregistrement est

AAAA Z

où

AAAA représente le code d'événements, et

Z représente un identificateur séparé du code d'événements par au moins un espace.

B.3.5 Si on utilise le traçage en couleur, les couleurs et les autres caractéristiques peuvent être indiquées par un groupe de caractères après un point (.) comme identificateur de groupe. La signification des caractères dépendrait de l'application particulière.

B.4.1 Les enregistrements de désignation comprennent l'enregistrement du nom de l'événement, du titre et des notes qui commentent les événements de base. Bien qu'il ne soit pas obligatoire de désigner tous les événements, le fichier de description de l'arbre de défaillances doit contenir un nombre suffisant d'enregistrements de désignation pour que l'arbre soit bien compris. Dans le cas des portes M1, un enregistrement du nom de l'événement est obligatoire.

B.4.2 L'enregistrement du nom de l'événement se présente ainsi:

AAAA 'xxxx xx xxx;zz z zzzz

où

AAAA représente le code d'événements;

l'apostrophe (') est séparée du code d'événements par au moins un espace;

xxxx xx xxx représente la première ligne du nom de l'événement.

Le nom de l'événement (description) commence immédiatement après l'apostrophe et peut contenir jusqu'à 40 caractères ASCII imprimés. Le point-virgule (;) sert à mettre fin à la première des deux lignes du traçage d'un nom étalé sur deux lignes comprenant un maximum de 20 caractères chacune.

B.4.3 L'enregistrement du titre indique le titre et se présente de la même façon que l'enregistrement du nom de l'événement; on le distingue de ce dernier par sa position devant tout enregistrement de désignation ou de description de base. Le code d'événements de l'enregistrement du titre peut être soit le code d'un événement de l'arbre de défaillances (auquel cas l'enregistrement du titre sert aussi d'enregistrement du nom de l'événement), soit un code factice dont la fonction n'est que de satisfaire aux exigences de la présentation.

B.4.4 L'enregistrement d'une note à un événement de base se présente de la même manière que l'enregistrement du nom de l'événement, sauf qu'on utilise comme identificateur les deux-points (:) plutôt que l'apostrophe (').

B.5.1 Les enregistrements auxiliaires facilitent le traitement du fichier de description de l'arbre de défaillances, y compris l'introduction, le traitement et la mise en mémoire dans la base de données des arbres de défaillances. Les enregistrements auxiliaires comprennent les commentaires et les enregistrements accompagnés de substituts de préfixe.

B.5.2 Un enregistrement précédé d'un astérisque (*) dans la première colonne est identifié comme un enregistrement de commentaire et ne sert pas au traitement de l'arbre de défaillances. Les commentaires qui précèdent le premier enregistrement traité apparaissent sur le terminal durant le traitement interactif, ou sont insérés au début du fichier de sortie, si l'arbre de défaillances est traité par lots.

B.5.3 Un enregistrement de définition de substitut de préfixe comprend une esperluète (&) dans la première colonne, suivie, après au moins un espace, du symbole d'égalité (=) lui-même suivi de deux à six caractères indiquant le préfixe. Dans les enregistrements ultérieurs, en cas de référence aux événements dotés d'un tel préfixe, le préfixe peut être remplacé par une esperluète (&) qui sert alors de premier caractère. Pour former le code complet, l'ordinateur remplace le substitut de préfixe par le groupe de deux à six caractères déjà défini. Le substitut de préfixe peut être redéfini par un nouvel enregistrement définissant un substitut de préfixe, ou il peut être annulé par un enregistrement ayant des blancs après le symbole d'égalité.

B.6 Parmi les enregistrements arbitraires, mentionnons les cartes paramètres de contrôles exigés par certains centres d'informatique et les enregistrements contenant des renseignements supplémentaires indispensables à certains programmes de traitement des arbres de défaillances, telle la définition d'options de programme. Les enregistrements arbitraires doivent comprendre, soit un seul groupe de caractères, soit plusieurs groupes dont le premier doit contenir une virgule (,). L'ordre des enregistrements arbitraires est fonction de l'exigence du programme qui commande l'utilisation de ces enregistrements. Les fichiers soumis à la CCEA peuvent comprendre des enregistrements arbitraires n'ayant aucune signification.

B.7 Les combinaisons d'enregistrements suivantes peuvent être employées pour faciliter la gestion du fichier de description d'un arbre de défaillances:

(a) un enregistrement Z combiné avec un enregistrement du nom de l'événement (B.4.1) où Z doit se trouver entre le code d'événements et l'apostrophe ('), séparé par au moins un espace:

```
AAAA Z 'xxx xx xxx'zzzz z zz
```

(b) Un enregistrement Z combiné avec un enregistrement de description d'un événement de base (B.3.3) où Z doit suivre l'indicateur de symbole, séparé par au moins un espace:

```
AAAA T Z #xxx
```

(c) Un enregistrement de description d'un événement de base (y compris celui associé à un enregistrement Z tel que défini ci-dessus) combiné avec un enregistrement de nom:

```
AAAA T Z #xxx 'xxx xx xxxx;zzzz z zz
```

B.8 Si certains programmes d'analyse d'arbres de défaillances nécessitent des données supplémentaires, celles-ci peuvent être introduites au moyen d'un groupe de données en utilisant comme identificateur un trait d'union (-) ou le symbole du pourcentage (%). La présentation utilisée est analogue à celle de l'enregistrement de nom. Ces groupes de données supplémentaires ne doivent pas contenir d'apostrophes (') ou de deux-points (:), et lorsqu'il s'agit d'enregistrements combinés, ils doivent précéder le nom ou le commentaire.